

(51) Int.Cl. ⁷	識別記号	F I	テグコード (参考)
H 0 4 L 12/66		H 0 4 L 12/66	B 5 B 0 8 9
G 0 6 F 13/00	3 5 1	G 0 6 F 13/00	3 5 1 Z 5 K 0 3 0

審査請求 未請求 請求項の数10 O L (全 24 頁)

(21) 出願番号 特願2000-382597(P2000-382597)

(22) 出願日 平成12年12月15日 (2000. 12. 15)

(71) 出願人 000005223

富士通株式会社

神奈川県川崎市中原区小田中4丁目1番
1号

(72) 発明者 安藤 忠直

神奈川県横浜市港北区新横浜3丁目9番18
号富士通コミュニケーション・システムズ
株式会社内

(74) 代理人 100089244

弁理士 遠山 勉 (外1名)

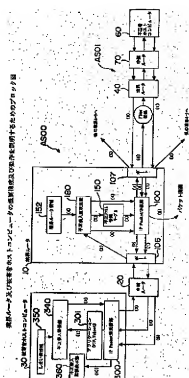
最終頁に続く

(54) 【発明の名称】 不正侵入防御機能を有するIP通信ネットワークシステム

(57) 【要約】

【課題】 他のキャリア（他のプロバイダ）のIPネットワーク、つまり自律システムを介して侵入してきた不正者を1つ1つの中継箇所を逆上り特定せず、直接境界箇所にて検出することで不正者を高速に（短時間に）特定し、遮断する。

【解決手段】 IP通信ネットワークシステムは、それぞれ独立のドメインのIPネットワークを構成し、かつIPパケットのインテリア伝送及びエクステリア伝送を行う複数の自律システムを備えるIP通信ネットワークシステムであって、前記複数の自律システムのそれぞれの前記IPネットワークの境界箇所位置する複数の境界中継装置のそれぞれは、伝送されてきた前記IPパケットが不正侵入の不正パケットである場合、前記不正パケットの再侵入を検出するためのフィルタリング情報に基づいて前記再侵入を検出したときは、前記不正パケットを廃棄する廃棄手段と、前記フィルタリング情報を同一自律システム内の他の全ての前記境界中継装置に配布する配布手段とを有する。



【特許請求の範囲】

【請求項1】 それぞれ独立のドメインのIPネットワークを構成し、かつIPパケットのインテリア伝送及びエクステリア伝送を行う複数の自律システムを備えるIP通信ネットワークシステムであって、前記複数の自律システムのそれぞれの前記IPネットワークの境界個所に位置する複数の境界中継装置のそれぞれは、伝送されてきた前記IPパケットが不正侵入の不正パケットである場合、

前記不正パケットの再侵入を検出するためのフィルタリング情報に基づいて前記再侵入を検出したときは、前記不正パケットを廃棄する廃棄手段と、前記フィルタリング情報を同一自律システム内の他の全ての前記境界中継装置に配布する配布手段とを有するIP通信ネットワークシステム。

【請求項2】 前記複数の自律システムのそれぞれのホストコンピュータは、伝送されてきた前記IPパケットが不正侵入の不正パケットであることを予め定められた判定情報に基づいて検出する検出手段を有する請求項1記載のIP通信ネットワークシステム。

【請求項3】 前記境界中継装置の前記配布手段は、前記フィルタリング情報を前記不正パケットを伝送してきた対向の前記自律システム内の前記境界中継装置に更に配布する請求項1または2記載のIP通信ネットワークシステム。

【請求項4】 前記複数の自律システムのそれぞれの前記IPネットワークの中継個所に位置する複数の中継装置のそれぞれは、伝送されてきた前記IPパケットが不正侵入の不正パケットである場合、

前記不正パケットの再侵入を検出するためのフィルタリング情報に基づいて前記再侵入を検出したときは、前記不正パケットを廃棄する廃棄手段と、前記フィルタリング情報を同一自律システム内の他の全ての前記中継装置に配布する配布手段とを有する請求項1、2または3記載のIP通信ネットワークシステム。

【請求項5】 独立のドメインのIPネットワークを構成し、かつIPパケットのインテリア伝送及びエクステリア伝送を行う自律システムの境界個所に位置し、伝送されてきた前記IPパケットが不正侵入の不正パケットである場合、

前記不正パケットの再侵入を検出するためのフィルタリング情報に基づいて前記再侵入を検出したときは、前記不正パケットを廃棄する廃棄手段と、前記フィルタリング情報を前記自律システム内の他の全ての境界中継装置に配布する配布手段とを有する境界中継装置。

【請求項6】 前記配布手段は、前記フィルタリング情報を前記不正パケットを伝送してきた対向の前記自律シ

ステム内の境界個所に位置する境界中継装置に更に配布する請求項5記載の境界中継装置。

【請求項7】 それぞれ独立のドメインのIPネットワークを構成し、かつIPパケットのインテリア伝送及びエクステリア伝送を行う複数の自律システムを備えるIP通信ネットワークシステムにおいて、前記複数の自律システムのそれぞれは、伝送されてきた前記IPパケットが不正侵入の不正パケットであることを予め定められた判定情報に基づいて検出するステップと、

前記IPネットワークの一つの境界個所で、前記不正パケットの再侵入を検出するためのフィルタリング情報に基づいて前記再侵入を検出したとき、前記不正パケットを廃棄するステップと、前記フィルタリング情報を同一自律システム内の他の全ての境界個所に配布するステップとを有する不正侵入防御方法。

【請求項8】 前記フィルタリング情報を前記不正パケットを伝送してきた対向の前記自律システム内の境界個所に配布するステップを更に有する請求項7記載の不正侵入防御方法。

【請求項9】 前記複数の自律システムのそれぞれは、伝送されてきた前記IPパケットが不正侵入の不正パケットである場合、

前記IPネットワークの一つの中継個所で、前記不正パケットの再侵入を検出するためのフィルタリング情報に基づいて前記再侵入を検出したときは、前記不正パケットを廃棄するステップと、前記フィルタリング情報を同一自律システム内の他の全ての境界個所に配布するステップとを更に有する請求項7または8記載の不正侵入防御方法。

【請求項10】 独立のドメインのIPネットワークを構成し、かつIPパケットのインテリア伝送及びエクステリア伝送を行う自律システムの境界個所において、伝送されてきた前記IPパケットが不正侵入の不正パケットである場合、

前記不正パケットの再侵入を検出するためのフィルタリング情報に基づいて前記再侵入を検出したときは、前記不正パケットを廃棄するステップと、前記フィルタリング情報を前記自律システム内の他の全ての境界個所に配布するステップとを有する不正侵入防御方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は不正行為防止機能を有するIP(Internet Protocol)通信ネットワークシステムに関し、特にインターネットにおける自律システム(AS:Autonomous System)のホストコンピュータに対する悪意のデータ通信を探知(追跡)し、不正行為を防止することを可能にするIP通信ネットワークシステムに関

する。

【0002】

【従来の技術】国際的な規模のIPネットワークであるインターネットにおいて発生する不正行為（以下、不正アクセスと記載することもある）に対して、この不正行為の発信元を特定して自動的に遮断することにより、不正行為者（以下、単に不正者と記載することもある）からホストコンピュータ及びインターネットを保護する必要がある。

【0003】この不正行為としては、例えば、故意に大量の無効パケットを特定のホストコンピュータに送信して、ホストコンピュータの機能停止を生じさせるDOS攻撃（サービス停止攻撃：Denial of Service Attack）や、他人のパスワードを不正に入手するために、パスワードを変えさせながら何度もホストコンピュータにアクセスを行う行為がある。

【0004】インターネットなどのIPネットワークでは、データをパケットの形態で伝送（転送、交換を含む）するので、IPパケットがどのネットワーク中継装置（以下、単に中継装置と記載することもある）を経由して到着したかを探索することにより、不正者を特定することができる。

【0005】不正者特定のために、ネットワーク中継装置に残されたIPパケットのログと不正行為による侵入の時刻とを対比しながらIPネットワーク内のパケットの侵入経路を探索する手法がある。

【0006】また、不正行為による侵入を防ぐために、外部ネットワークとの間にファイアウォールと呼ばれる特別なコンピュータを備え、フィルタリング技術を用いて特定のパケット（特定のアドレスやサービスポート）を制限し、ホストコンピュータ及びIPネットワークを防護する手法がある。

【0007】さらに、次に示すような2つの従来技術がある。第1の技術は、Cisco社製のNet Ranger（登録商標）である。Net Rangerの概念図を示す図1を参照すると、このシステムにおいては、不正者がIPネットワークを介してホストコンピュータ（HOST）3に不正アクセスにより侵入した場合、そのホストコンピュータ3に付属している不正監視装置（侵入検知ツール）4はネットワークの接続性を検査するためのloginやpingのしきい値を判定したり、操作パターン特徴認識（成り済まし検索）を実施して異常を検出する。

【0008】不正監視装置4は、ルータ1及びファイアウォール2に対して異常検出を通知し、不正アクセスの被害対象となっているホストコンピュータ3への接続を遮断するためのフィルタテーブル5の作成をルータ1及びファイアウォール2に依頼する。

【0009】このフィルタテーブル5が作成されたことで、再度の侵入があっても、ホストコンピュータ5の前

段でフィルタリングによりパケットを廃棄することにより、不正者はホストコンピュータ5に対して攻撃を行えなくなる。

【0010】第2の技術は、特開2000-124952号公報記載のデータ追跡システムである。このデータ追跡システムの概念図を示す図2を参照すると、このシステムにおいては、不正アクセス者6がIPネットワークを介してホストコンピュータ9Aに侵入してきた場合、そのホストコンピュータ9Aに付属している不正アクセスの事実を検出する装置9Bが不正を検出し、付随している管理システム9Cに通知する。

【0011】管理システム9Cは検出装置9Bの前段の中継装置7Cに対し、不正アクセスの発信元の追跡を依頼する。追跡依頼を受信した中継装置7Cは不正アクセス者6の特微情報と自身が中継するデータとを比較する機能をもち、不正データを検出した場合にはその不正データ内のデータリンク層の解析8Cに基づいて、その不正データを発信した1つ前段の中継装置7Bを検出することができる。

【0012】中継装置7Cは特定した中継装置7Bに不正発信元の追跡を依頼すると同時に、管理システム9Cに特定した前段の中継装置7Bの情報を通知する。このような機能をもつ中継装置7A、7B、7C（データリンク層の解析8A、8B、8Cを含む）を連鎖的にネットワークに設置することにより、最終的に不正アクセス者6の発信元を特定できる。

【0013】このシステムにおいては、不正アクセス者6が特定された場合、その不正アクセス者6に警告を発すると共に、ネットワーク管理者に通知が行われる。

【0014】

【発明が解決しようとする課題】不特定多数の個人ユーザ及び企業ユーザが自由にIPネットワークを利用できるIP通信ネットワークシステムでは、IPネットワーク全体のどこからでも不正行為が行われる危険性を有する。

【0015】上述した従来の技術では、比較的小規模なIPネットワークでの不正者検出と侵入の防護とが可能であるものの、国際的な規模のIPネットワークでは十分な効力を発揮しない。

【0016】つまり、従来の技術においては、前述した例のように、故意に大量のIPパケットを送信するような不正行為の場合、ファイアウォール等でフィルタリングを行いホストコンピュータの防護を行えるものの、大量不正パケットによりIPネットワーク全体へのトラフィックが増加し、通常のパケット制御に悪影響を与えることを免れない。

【0017】また、不正アクセスを検出し不正者を特定するためには、不正者に至るまでの中継装置（ルータ）を1つずつ逆上らなくてはならず、多数の中継装置が経路中に介在するインターネットでは、不正者を特定する

には多大な時間を要する。

【0018】さらに、インターネットにおいては頻繁に経路の変更が行なわれており、中継装置を逆上る手法では、経路変更が行なわれた場合には始めから追跡をやり直さなければならなくなる可能性がある。

【0019】本発明の課題は、これらの従来技術の問題を解決し、不正パケットの再侵入の遮断を高速に可能とするIP通信ネットワークシステム及び手法を提供することにある。

【0020】

【課題を解決するための手段】上記課題を解決するために、本発明の第1のIP通信ネットワークシステムは、それぞれ独立のドメインのIPネットワークを構成し、かつIPパケットのインテリア伝送及びエクステリア伝送を行う複数の自律システムを備えるIP通信ネットワークシステムであって、前記複数の自律システムのそれぞれの前記IPネットワークの境界個所に位置する複数の境界中継装置のそれぞれは、伝送されてきた前記IPパケットが不正侵入の不正パケットである場合、前記不正パケットの再侵入を検出するためのフィルタリング情報に基づいて前記再侵入を検出したときは、前記不正パケットを廃棄する廃棄手段と、前記フィルタリング情報を同一自律システム内の他の全ての前記境界中継装置に配布する配布手段とを有する。

【0021】本発明の第2のIP通信ネットワークシステムは、前記複数の自律システムのそれぞれのホストコンピュータは、伝送されてきた前記IPパケットが不正侵入の不正パケットであることを予め定められた判定情報に基づいて検出する検出手段を有する。

【0022】本発明の第3のIP通信ネットワークシステムは、前記境界中継装置の前記配布手段は、前記フィルタリング情報を前記不正パケットを伝送してきた対向の前記自律システム内の前記境界中継装置に更に配布する。

【0023】本発明の第4のIP通信ネットワークシステムは、前記複数の自律システムのそれぞれの前記IPネットワークの中継個所に位置する複数の中継装置のそれぞれは、伝送されてきた前記IPパケットが不正侵入の不正パケットである場合、前記不正パケットの再侵入を検出するためのフィルタリング情報に基づいて前記再侵入を検出したときは、前記不正パケットを廃棄する廃棄手段と、前記フィルタリング情報を同一自律システム内の他の全ての前記中継装置に配布する配布手段とを有する。

【0024】本発明の第1の境界中継装置は、独立のドメインのIPネットワークを構成し、かつIPパケットのインテリア伝送及びエクステリア伝送を行う自律システムの境界個所に位置し、伝送されてきた前記IPパケットが不正侵入の不正パケットである場合、前記不正パケットの再侵入を検出するためのフィルタリング情報に

基づいて前記再侵入を検出したときは、前記不正パケットを廃棄する廃棄手段と、前記フィルタリング情報を前記自律システム内の他の全ての境界中継装置に配布する配布手段とを有する。

【0025】本発明の第2の境界中継装置は、前記配布手段は、前記フィルタリング情報を前記不正パケットを伝送してきた対向の前記自律システム内の境界個所に位置する境界中継装置に更に配布する。

【0026】本発明の第1の不正侵入防御方法は、それぞれ独立のドメインのIPネットワークを構成し、かつIPパケットのインテリア伝送及びエクステリア伝送を行う複数の自律システムを備えるIP通信ネットワークシステムにおいて、前記複数の自律システムのそれぞれは、伝送されてきた前記IPパケットが不正侵入の不正パケットであることを予め定めた判定情報に基づいて検出するステップと、前記IPネットワークの一つの境界個所で、前記不正パケットの再侵入を検出するためのフィルタリング情報に基づいて前記再侵入を検出したとき、前記不正パケットを廃棄するステップと、前記フィルタリング情報を同一自律システム内の他の全ての境界個所に配布するステップとを有する。

【0027】本発明の第2の不正侵入防御方法は、前記フィルタリング情報を前記不正パケットを伝送してきた対向の前記自律システム内の境界個所に配布するステップを更に有する。

【0028】本発明の第3の不正侵入防御方法は、前記複数の自律システムのそれぞれは、伝送されてきた前記IPパケットが不正侵入の不正パケットである場合、前記IPネットワークの一つの中継個所で、前記不正パケットの再侵入を検出するためのフィルタリング情報に基づいて前記再侵入を検出したときは、前記不正パケットを廃棄するステップと、前記フィルタリング情報を同一自律システム内の他の全ての境界個所に配布するステップとを更に有する。

【0029】本発明の第4の不正侵入防御方法は、独立のドメインのIPネットワークを構成し、かつIPパケットのインテリア伝送及びエクステリア伝送を行う自律システムの境界個所において、伝送されてきた前記IPパケットが不正侵入の不正パケットである場合、前記不正パケットの再侵入を検出するためのフィルタリング情報に基づいて前記再侵入を検出したときは、前記不正パケットを廃棄するステップと、前記フィルタリング情報を前記自律システム内の他の全ての境界個所に配布するステップとを有する。

【0030】

【発明の実施の形態】次に、本発明の実施の形態について図面を参照して説明する。

【0031】[IP通信ネットワークシステムの全体構成] 本発明の一実施の形態におけるIP通信ネットワークシステムの全体構成を示す図3を参照すると、このシ

システム S Y S は I P ネットワークとしてのインターネットに適用される。

【0032】 I P 通信ネットワークシステム S Y S には、複数の自律システム A S O O, A S O 1, A S O 2 が存在する。自律システム A S O O, A S O 1, A S O 2 のそれぞれはドメインまたは内部システムとも称され、1つのインターネット接続事業者（プロバイダ）または企業のエントラネットなどが該当する。自律システム A S O O, A S O 1, A S O 2 のそれぞれは、独立のドメインの I P ネットワークを構成し、かつ I P パケットのインテリア伝送及びエクステリア伝送を行う。

【0033】 自律システム A S O O, A S O 1, A S O 2 の相互間は境界ルータ R T 1 と呼ばれるゲートウェイ（ネットワーク中継装置）を通して接続されている。各自律システム A S O O, A S O 1, A S O 2 において、境界ルータ R T 1 間には中継ルータ R T 2 を通じて接続されている。各中継ルータ R T 2 はホストコンピュータを収容することができる。また、ホストコンピュータには複数のユーザ端末装置（パーソナルコンピュータなど）が接続可能である。

【0034】 ここに示す例では、自律システム A S O O 内の中継ルータ（R T 2）20に被害者ホストコンピュータ 30 が収容され、自律システム A S O 1 内の中継ルータ（R T 2）70 に不正者ホストコンピュータ 60 が収容されている。自律システム A S O O と自律システム A S O 1 とは、境界ルータ（R T 1）10, 40 を通じて接続されている。

【0035】 このような I P 通信ネットワークシステム S Y S において、不正者ホストコンピュータ 60 の追跡を難しくしている背景には、複数の自律システム A S O O, A S O 1 における多数のルータ（R T 1, R T 2）10, 20, 40, 70 を経由して不正者ホストコンピュータ 60 から被害者ホストコンピュータ 30 に不正パケットが到達するためである。

【0036】 しかし、後に詳述するように、各境界ルータ R T 1 に特別な機構を配備することにより、不正パケットの発信元の追跡と、不正パケットの再侵入の遮断とが高速に可能となる。

【0037】 [境界ルータ及び被害者ホストコンピュータの概要構成及び動作] 次に、図3に示す I P 通信ネットワークシステム S Y S における自律システム A S O O に配置された境界ルータ 10 及び被害者ホストコンピュータ 30 の構成及び動作の概要について説明する。

【0038】 図3及び図4を参照すると、自律システム A S O 1 内の図示省略の不正者端末装置が接続されているホストコンピュータ（不正者）60 から不正アクセスのパケットが送信された場合、この不正アクセスパケットは中継ルータ 70 及び境界ルータ 40 を通じて、自律システム A S O O の境界ルータ 10 に到達する。

【0039】 境界ルータ 10 に到達した不正アクセスパ

ケットは、境界ルータ 10 内の I P パケット中継部 100 を通過した後、中継ルータ 20 を通ってホストコンピュータ（被害者）30 の I P パケット送受信部 300 に受信される。

【0040】 不正アクセスパケットは更に T C P / I P (Transmission Control Protocol over Internet Protocol) 階層のアプリケーションプロトコル（以下、単にアプリケーションと記載する）301 を介して不正侵入監視部 340 に渡される（動作手順 O P 1）。

【0041】 次に、不正侵入監視部 340 は、しきい値情報 350 を参照し、予め定められたしきい値を超えている場合、不正アクセスがあったことを示す不正アクセス発生情報（後に詳述する探索要求データ）を I P パケット送受信部 300 に通知する。しきい値情報 350 の設定はホストコンピュータ 30 の管理者によって予め行われる。

【0042】 I P パケット送受信部 300 から送信された不正アクセス発生情報は、中継ルータ 20 を介して境界ルータ 10 のポート 106 に入力され、不正侵入監視装置 180 に通知される。なお、厳密には、不正アクセス発生情報はポート 106 から I P パケット中継部 100 を経由して不正侵入監視装置 180 に通知される（O P 2）。

【0043】 不正侵入監視装置 180 は受信した不正アクセス発生情報に基づく不正アクセス情報を不正アクセス情報テーブル 150 に登録する（O P 3）。また、不正侵入監視装置 180 は境界ルータ情報 152 を参照し、情報配付先を決定する（O P 4）。

【0044】 境界ルータ 10 は不正アクセス情報テーブル 150 の内容を自己の自律システム A S O 0 及び隣接する他の自律システム A S O 1 の他の境界ルータ R T 1, 40 に通知し、それぞれの境界ルータ内の不正アクセス情報テーブルに登録依頼する（O P 5）。

【0045】 この後、自律システム A S O 1 の不正者ホストコンピュータ 60 からの再侵入があると、不正アクセスパケットはポート 107 を通じて I P パケット中継部 100 に入る（O P 6）。I P パケット中継部 100 は不正アクセス情報テーブル 150 を参照し、受信した不正アクセスパケットの内容と比較する（O P 7）。

【0046】 この比較結果、内容が一致したならば、I P パケット中継部 100 において該当パケットを廃棄し、不正アクセスを遮断する（O P 8）。

【0047】 これにより、自律システム A S O O の境界ルータ 10 と隣接する他の自律システム A S O 1 の境界ルータ 40 との間で不正アクセス情報テーブル 150 の内容の交換ができ、不正者の侵入経路を高速に探索できるばかりでなく、不正アクセスパケットの侵入を自律システム A S O O などの自律ネットワーク単位で防御することができる。

【0048】 さらに、被害者ホストコンピュータ 30 に

において不正者の監視状況を把握するために、次の動作を行う。

【0049】つまり、上記動作手順OP3において、不正侵入監視装置180が不正監視状態になり、かつ上記動作手順OP8において、IPパケット中継部100が不正アクセスパケットを発見したとき、境界ルータ10、40、RT1のそれぞれの状況（後に詳述する不正侵入レスポンスデータ）をホストコンピュータ30に報告する（OP9）。

【0050】また、ホストコンピュータ30のIPパケット送受信部300は、報告された境界ルータ10、40、RT1のそれぞれの状況情報を不正侵入監視表示部360に伝達し、不正監視の状況表示を行わせる（OP10）。

【0051】〔境界ルータ及び被害者ホストコンピュータの詳細構成及び動作〕次に、図3及び図4に示すIP通信ネットワークシステムSYSにおける自律システムAS00に配置された境界ルータ10及び被害者ホストコンピュータ30の構成及び動作の詳細について説明する。

【0052】（被害者ホストコンピュータにおける不正者侵入時の処理）図15及び図16は被害者ホストコンピュータ30における不正者侵入時の処理手順を示している。

【0053】図5及び関連図を併せ参照すると、自律システムAS01内の不正者ホストコンピュータ60から不正アクセスのIPパケットが送信された場合、この不正アクセスパケット（以下、単に不正パケットと称することもある）は中継ルータ70及び境界ルータ40を通して、自律システムAS00の境界ルータ10に到達する。

【0054】境界ルータ10に到達した不正アクセスパケットは、境界ルータ10内のポート107、IPパケット中継部100、及びポート106を通過した後、中継ルータ20を通過して被害者ホストコンピュータ（HOST）30のIPパケット送受信部300に受信される。

【0055】不正アクセスパケットは更にアプリケーション301を介して不正侵入監視部340に渡される。つまり、TCP/IP階層のFTP（File Transfer Protocol）及びTelnet（Telecommunication Network Protocol）などのアプリケーション301では、不正アクセスを判断するのに必要な情報として、アプリケーション種別、セッション（session）情報、不正者のIPアドレス（偽りアドレス）、メッセージ種別、ユーザID、転送ファイル名、転送ファイルサイズ、操作ディレクトリ、及び入力コマンド名などを不正侵入監視部340の受付部302に送信して不正侵入監視機能を起動する。

【0056】不正侵入監視部340は起動されると、し

きい情報テーブル（図示省略）のしきい情報350に基づいて、不正侵入か否かの判断を行う。不正侵入監視部340の不正アクセス判定処理部303は、図16に示す処理手順に基づいて、アプリケーション301から受付部302を通して受信したアプリケーション種別やセッション情報などから、同一ユーザによる同一コマンド等の繰り返し攻撃なのか、単にトラフィックが上がっているのかを見極めたうえでしきい情報350と比較する。

【0057】しきい情報350には、図8に示すように、不正アクセスを監視するための種別（アプリケーション種別、メッセージ種別など）、それらに対応した不正トライ回数とが設定されている。しきい情報350は、図13に示すように、不正を監視するための各々の判定種別に対して複数の要素（条件）を保有し、それぞれの要素が全て満たされたときに不正となるように登録されている。

【0058】これにより、不正アクセスパケット検出の正確性を強化している。しきい情報350の設定は、被害者ホストコンピュータ30の管理者がその利用状況に応じて、コマンド163の入力により予め設定しておく。

【0059】より好ましくは、不正アクセスによる不正侵入を防ぐためのしきい情報350のほかに、ウィルスの特徴情報を設定できるようにすることで、ウィルスデータを含むパケットを送受信しないように、ホストコンピュータ30の不正侵入監視部340を構成する。

【0060】不正侵入監視部340の不正アクセス判定処理部303は、不正アクセスと判断すると、要求種別「登録（不正アクセス防止依頼要求）」を含む探索要求データ50を作成し、パケットの形態でIPパケット送受信部300及び中継ルータ20を経て、境界ルータ10に通知する。

【0061】探索要求データ50は、図6に一例を示すように、宛先ルータ（境界ルータ）IPアドレス、自ルータIPアドレス、宛先（被害者ホストコンピュータ30）IPアドレス、プロトコル種別、ポート番号などを一情報として含む。

【0062】（境界ルータにおける不正者情報配布時の処理）図17、図18及び図19は境界ルータにおける不正者情報（探索要求データ）配布時の処理手順を示している。

【0063】被害者ホストコンピュータ30から探索要求データ50により不正アクセス発生の通知を受けた境界ルータ10においては、ポート106からIPパケット中継部100を通して、不正侵入監視装置180の受付処理部104が起動される。

【0064】不正侵入監視装置180では、情報登録処理部103が探索要求データ50に含まれている不正者情報の内、被害者ホストコンピュータ30に対応する宛

先IPアドレス、プロトコル種別、及びポート番号を不正アクセス情報80(図7参照)として不正アクセス情報テーブル150に登録(追加登録)する。また、IPパケット送受信部103は探索要求データ50をアプリケーション301及び不正侵入レスポンス処理部109に送信する。これにより、この境界ルータ10は不正者ホストコンピュータ60から被害者ホストコンピュータ30への不正アクセスパケットの監視状態になる。

【0065】なお、不正アクセスの監視期間(時間)を予めコマンド162により情報登録処理部103に設定することも可能である。この場合には、所定の監視期間が満了すると不正監視を停止させるために、情報登録処理部103が不正アクセス情報テーブル150から該当する情報を削除する。

【0066】境界ルータ10の不正侵入レスポンス処理部109は、IPパケット送受信部103からの探索要求データ50に基づき、不正者ホストコンピュータ60の監視状態になっていることをIPパケット中継部100を通して宛先ホストコンピュータ、つまり被害者ホストコンピュータ30に伝達するために、レスポンス種別として「不正監視」を含む不正侵入レスポンスデータ140をパケット形態で送信する。

【0067】この不正侵入レスポンスデータ140には、図12に示すように、レスポンス種別としての「不正発見」及び「不正監視」の情報のはかに、宛先IPアドレス、自ルータIPアドレス、プロトコル種別、ポート番号、及び自ルータAS番号が含まれている。

【0068】情報登録処理部103による不正者アクセス情報テーブル150への不正監視を実施させるための不正アクセス情報80の登録が完了した後、宛先検索処理部102は境界ルータ情報テーブル151を検索し、不正アクセス情報通知先(境界ルータIPアドレス)を読み出す。この境界ルータ情報テーブル151には、図9に示すように、同一自律システムAS00内の境界ルータRT1のIPアドレスなどの境界ルータ情報152が登録されており、その宛先全ての境界ルータRT1に探索要求データ50が追跡依頼情報配付処理部101、IPパケット中継部100、及びポート107を通して通知される。

【0069】ここで、追跡依頼情報配付処理部101は宛先検索処理部102から受信した探索要求データ50のうちの宛先ルータIPアドレス及び自ルータIPアドレスを取得した境界ルータIPアドレス及び自境界ルータIPアドレスにそれぞれ更新する。また、追跡依頼情報配付処理部101は更新した探索要求データ50を記録する処理を取得アドレス数に対応する回数繰り返す。

【0070】境界ルータ情報テーブル151には、コマンド160で境界ルータ情報152を設定できるが、自律システムAS00内の他の全ての境界ルータRT1に境界ルータ情報152の設定を実施するに手間がか

かる。このために、境界ルータ情報送受信処理部105が他の境界ルータRT1との間で定期的に境界ルータ情報152を交換する。

【0071】以上の処理により、不正侵入された自律システムAS00内の全ての境界ルータRT1に、配布された探索要求データ50に基づく不正アクセス情報80が設定され、自律システムAS00全体が不正侵入の監視下におかれる状態になる。

【0072】(境界ルータにおける不正アクセスパケット監視時の処理)図20、図21及び図22は境界ルータにおける不正アクセスパケット監視時の処理手順を示している。

【0073】この状態で、更に自律システムAS01の境界ルータ40を通して不正アクセスがあった場合、不正者ホストコンピュータ60からのIPパケット(不正アクセスパケット)は、境界ルータ10のポート107を経由してIPパケット中継部100に送られる。

【0074】IPパケット中継部100は不正アクセス情報テーブル150を参照し、入力IPパケットが不正者ホストコンピュータ60からの不正アクセスパケットと一致するか否かを確認する。ここでは、不正者ホストコンピュータ60からの不正アクセスパケットのため、登録内容と一致する。

【0075】IPパケット中継部100は境界ルータ40から受信したIPパケット及び不正アクセス情報テーブル150に登録されている不正アクセス情報80を基に、図11に示す情報を含む不正パケット情報120を作成し、不正侵入監視装置180の宛先検索処理部102に送信する。

【0076】宛先検索処理部102は、不正アクセスパケットがどのルータから到来したのかを解析するために、不正パケット情報120と接続ルータ情報テーブル108内の接続ルータ情報90(図10参照)とを参照し、一致する近隣のルータのIPアドレス(不正アクセスパケットの送信元ルータIPアドレス)を取得する。なお、接続ルータ情報テーブル108への接続ルータ情報90は、予めコマンド160により、自ルータに接続されている近隣のルータの情報として登録される。

【0077】追跡依頼情報配付処理部101は宛先検索処理部102から取得したIPアドレス及び不正パケット情報120を基に、配布するべき境界ルータ40宛の探索要求データ50を作成する。この作成された探索要求データ50はIPパケット中継部100及びポート107を経由して境界ルータ40に送信される。

【0078】追跡依頼情報配付処理部101は、同時に、この境界ルータ10で不正アクセスパケットを発見したことを宛先ホストコンピュータ対応の被害者ホストコンピュータ30に伝達するために、レスポンス種別として「不正発見」を示した不正侵入レスポンスデータ140(図12参照)を不正侵入レスポンス処理部109

からIPパケット中継部100を經由して送信する。

【0079】自律システムA S O 1内の境界ルータ40は上述した処理を繰り返すことにより、自IPネットワーク内の不正者、つまりホストコンピュータ60を限定する。

【0080】探索要求データ50が最終的に不正者の存在する、厳密には不正者の使用する端末装置に係わるホストコンピュータ60に到達した場合、その不正者ホストコンピュータ60はルータ同様に不正者の判定を行い、不正者の情報を探索要求データ50の宛先IPアドレス対応の被害者ホストコンピュータ30に送信する。

【0081】不正者の特定が行われ、排除された後には、IPネットワーク全体の自律システムAS00、S01に登録解除を指示する必要がある。各境界ルータ50、40、RT1においては、通常は上述した監視期間（時間）によって登録解除を実施するが、コマンド161によって解除要求を境界ルータ10に送信し、不正アクセス情報テーブル150から該当する情報を削除することできる。

【0082】各境界ルータ10, 40, RT1から送信 20
された不正侵入レスポンスデータ140は、被害を受けて
いる被害者ホストコンピュータ30のIPパケット送
受信部300を経由して、不正侵入監視レスポンス受付
処理部304が受信し、不正侵入監視状況表示処理部3
05を起動する。

【0083】なお、不正侵入監視レスポンス受付処理部304及び不正侵入監視状況表示処理部305は、図4に示す被害者ホストコンピュータ30の不正侵入監視表示部360を構成する。

【0084】不正侵入監視状況表示処理部305は受信した不正侵入レスポンスデータ140からAS番号やルータアドレスを抽出し、図14に示すような不正侵入監視状況を不正侵入監視表示部360に表示する。

【0085】図14に示す不正侵入監視状況の表示例においては、A5番号「111」対応の自律システム内のマーク◎で記載したホストコンピュータ（IPアドレス：111.10.12.44）30が被害者であり、A5番号「2510」の自律システム内のマーク◇で記載した不正者ホストコンピュータ（IPアドレス：10.34.210.55）60が不正者の端末装置（IPアドレス：10.34.210.75）に係わることを示している。

【0086】また、各自律システムにおいてマーク●は「不正発見」の境界ルータを示し、マーク○は「不正監視中」の境界ルータを示している。

【００８７】以上説明したように、本発明の一実施の形態のＩＰ通信ネットワークシステムＳＹＳにおいては、インターネットなどのＩＰネットワークから自律システムＡＳ００のホストコンピュータ３０に侵入してきた不正者の不正アクセスパケットは、境界ルータ１０の不正

侵入監視装置180で検出し、同一自律システムASO0内の他の境界ルータRT1に通知する。

【0088】境界ルータ10では、自境界ルータの不正アクセス情報テーブル1510に直接登録し、再侵入時、高速で送信元のキャリア（プロバイダ）を特定することが可能。境界ルータ情報テーブル1511には、自律システムAS00内の境界ルータ10、RT1のIPアドレスが登録されており、この宛先に不正者情報（探索要求データ50）を配付することにより、不正者特定の高速化を図ることが可能になる。また、不正なパケットの侵入を自律システムAS00のネットワーク単位で防御できるように、不正アクセスパケットによるトラフィック増加などを防止できる。

【0089】各境界ルータ10、RT1に不正アクセス情報テーブル150をもち、再侵入してきた場合、その不正アクセス情報テーブル150内の不正アクセス情報80と比較し、該当する侵入者と判明したならば、送信ルータ(RT1)40に探索要求データ50を配付する。これを繰り返すことにより、不正者に最も近いルータ(RT1)40にたどり着いた場合には、そのルータにて遮断処理が行なわれ、不正者のアクセスを遮断することができる。

【0090】さらに、被害者ホストコンピュータ30の存在する自律システムAS00内の全ての他境界ルータRT1に情報が通知されているため、経路が変更された場合でも、迅速に探索を開始することが可能になる。

【００９１】〔変形例〕上述した一実施の形態のＩＰ通信ネットワークシステムにおいて、同一の自律システムの内部に不正者（不正者のホストコンピュータ及び端末装置）及び被害者（被害者ホストコンピュータ）が存在する場合は、上記境界ルータの機能を持つ中継ルータを自律システムの内部に配備することにより、不正者の特定を同様に行うことができる。

【0092】この場合、自律システム内の各々の中継ルータ内部の接続ルータ情報テーブル及び境界ルータ情報テーブルには、自ルータに接続されているルータを登録しておく。

【0093】不正を検出した被害者ホストコンピュータは探索要求データを境界ルータに送信すると共に、自被害者ホストコンピュータに接続している中継ルータにも送信する。中継ルータによる不正者特定の処理手法は上述した境界ルータによる不正者の特定手法と同じである。

【0094】〔付記〕

(付記1) それぞれ独立のドメインのIPネットワークを構成し、かつIPパケットのインテリア伝送及びエクステリア伝送を行う複数の自律システムを備えるIP通信ネットワークシステムであって、前記複数の自律システムのそれぞれの前記IPネットワークの境界個所に位置する複数の境界中継装置のそれぞれは、伝送されて

きた前記IPパケットが不正侵入の不正パケットである場合、前記不正パケットの再侵入を検出するためのフィルタリング情報に基づいて前記再侵入を検出したときは、前記不正パケットを廃棄する廃棄手段と、前記フィルタリング情報を同一自律システム内の他の全ての前記境界中継装置に配布する配布手段とを有するIP通信ネットワークシステム。

【0095】(付記2) 前記複数の自律システムのそれぞれのホストコンピュータは、伝送されてきた前記IPパケットが不正侵入の不正パケットであることを予め定められた判定情報に基づいて検出する検出手段を有する付記1記載のIP通信ネットワークシステム。

【0096】(付記3) 前記境界中継装置の前記配布手段は、前記フィルタリング情報を前記不正パケットを伝送してきた対向の前記自律システム内の前記境界中継装置に更に配布する付記1または2記載のIP通信ネットワークシステム。

【0097】(付記4) 前記複数の自律システムのそれぞれの前記IPネットワークの中継個所に位置する複数の中継装置のそれぞれは、伝送されてきた前記IPパケットが不正侵入の不正パケットである場合、前記不正パケットの再侵入を検出するためのフィルタリング情報に基づいて前記再侵入を検出したときは、前記不正パケットを廃棄する廃棄手段と、前記フィルタリング情報を同一自律システム内の他の全ての前記中継装置に配布する配布手段とを有する付記1、2または3記載のIP通信ネットワークシステム。

【0098】(付記5) 独立のドメインのIPネットワークを構成し、かつIPパケットのインテリア伝送及びエクステリア伝送を行う自律システム内の境界個所に位置し、伝送されてきた前記IPパケットが不正侵入の不正パケットである場合、前記不正パケットの再侵入を検出するためのフィルタリング情報に基づいて前記再侵入を検出したときは、前記不正パケットを廃棄する廃棄手段と、前記フィルタリング情報を前記自律システム内の他の全ての境界中継装置に配布する配布手段とを有する境界中継装置。

【0099】(付記6) 前記配布手段は、前記フィルタリング情報を前記不正パケットを伝送してきた対向の前記自律システム内の境界個所に位置する境界中継装置に更に配布する付記5記載の境界中継装置。

【0100】(付記7) それぞれ独立のドメインのIPネットワークを構成し、かつIPパケットのインテリア伝送及びエクステリア伝送を行う複数の自律システムを備えるIP通信ネットワークシステムにおいて、前記複数の自律システムのそれぞれの、伝送されてきた前記IPパケットが不正侵入の不正パケットであることを予め定めた判定情報に基づいて検出するステップと、前記IPネットワークの一つの境界個所で、前記不正パケットの再侵入を検出するためのフィルタリング情報に基づ

いて前記再侵入を検出したとき、前記不正パケットを廃棄するステップと、前記フィルタリング情報を同一自律システム内の他の全ての境界個所に配布するステップとを有する不正侵入防御方法。

【0101】(付記8) 前記フィルタリング情報を前記不正パケットを伝送してきた対向の前記自律システム内の境界個所に配布するステップを更に有する付記7記載の不正侵入防御方法。

【0102】(付記9) 前記複数の自律システムのそれぞれの、伝送されてきた前記IPパケットが不正侵入の不正パケットである場合、前記IPネットワークの一つの中継個所で、前記不正パケットの再侵入を検出するためのフィルタリング情報に基づいて前記再侵入を検出したときは、前記不正パケットを廃棄するステップと、前記フィルタリング情報を同一自律システム内の他の全てのの中継個所に配布するステップを更に有する付記7または8記載の不正侵入防御方法。

【0103】(付記10) 独立のドメインのIPネットワークを構成し、かつIPパケットのインテリア伝送及びエクステリア伝送を行う自律システム内の境界個所において、伝送されてきた前記IPパケットが不正侵入の不正パケットである場合、前記不正パケットの再侵入を検出するためのフィルタリング情報に基づいて前記再侵入を検出したときは、前記不正パケットを廃棄するステップと、前記フィルタリング情報を前記自律システム内の他の全ての境界個所に配布するステップとを有する不正侵入防御方法。

【0104】(付記11) 前記フィルタリング情報を前記不正パケットを伝送してきた対向の前記自律システム内の境界個所に配布するステップを有する付記10記載の不正侵入防御方法。

【0105】
【発明の効果】以上説明したように、本発明によれば、他のキャリア（他のプロバイダ）のIPネットワーク、つまり自律システムを介して侵入してきた不正者を1つ1つの中継個所を逆上り特定せず、直接境界個所にて検出することで不正者を高速に（短時間で）特定し、遮断することができる。

【0106】また、不正者情報（フィルタリング情報）を同一自律システム（同一キャリアネットワーク）内の全ての境界個所にもたすことで、その自律システム全体にガードがかかることになり、不正アクセスのIPパケットの再侵入を防ぐことができる。

【図面の簡単な説明】

【図1】従来のIP通信ネットワークシステムの第1の例を説明するための図。

【図2】従来のIP通信ネットワークシステムの第2の例を説明するための図。

【図3】本発明の一実施の形態のIP通信ネットワークシステムの構成を示すブロック図。

【図4】境界ルータ及び被害者ホストコンピュータの概要構成及び動作を説明するためのブロック図。

【図5】境界ルータ及び被害者ホストコンピュータの詳細構成及び動作を説明するためのブロック図。

【図6】探索要求データを説明するための図。

【図7】不正アクセス情報を説明するための図。

【図8】しきい値情報を説明するための図。

【図9】境界ルータ情報を説明するための図。

【図10】接続ルータ情報を説明するための図。

【図11】不正パケット情報を説明するための図。

【図12】不正侵入レスポンスデータを説明するための図。

【図13】しきい値情報の判定種別の要素を説明するための図。

【図14】不正侵入監視状況の表示例を示す。

【図15】被害者ホストコンピュータにおける不正者侵入時の処理を示すフローチャート。

【図16】被害者ホストコンピュータにおける不正者侵入時の処理を示すフローチャート。

10 理を示すフローチャート。

【図22】境界ルータにおける不正パケット監視時の処理を示すフローチャート。

【符号の説明】

SYS 1P 通信ネットワークシステム

AS00, AS01, AS02 自律システム

10, 40, RT1 境界ルータ

20, 70, RT2 中継ルータ

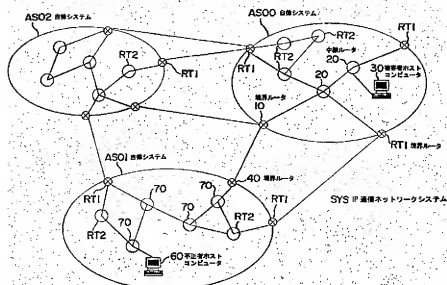
30 被害者ホストコンピュータ

60 不正者ホストコンピュータ

【図3】

【図6】

本発明の一実施形態の1P通信ネットワークシステムの構成を示すブロック図



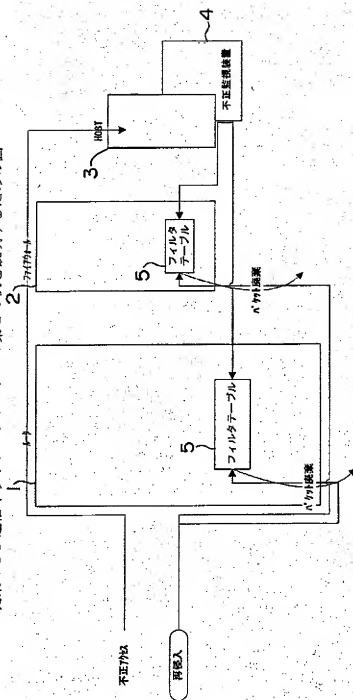
探索要求データを説明するための図

50

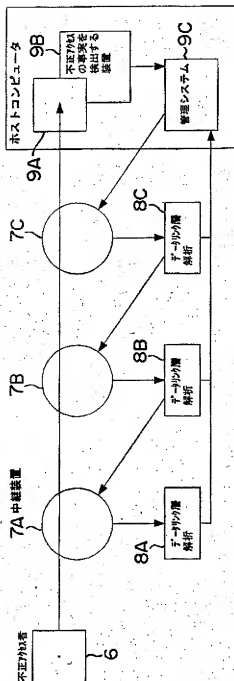
要求種別(発報/解除)
宛先→ IP address
自ル→ IP address
宛先 IP address
プロトコル種別
Port 番号

【図1】

従来のIP通信ネットワークシステムの第1の例を説明するための図



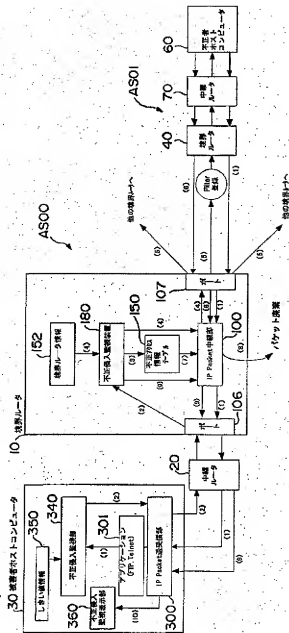
【図2】



従来のIP通信ネットワークシステムの第2の例を説明するための図

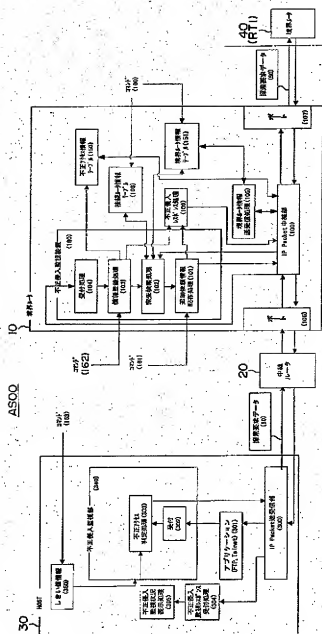
【図4】

境界ルータ及び拡張寄与ホストコンピュータの構成及び動作を説明するためのブロック図



【図5】

携帯メール及び携帯システムコンピュータの動作を説明するためのブロック図



【図7】

不正アクセス情報を説明するための図

80 不正アクセス情報

監視期間 (時間)
宛先 IP address
プロトコル種別
Port 番号

【図8】

しきい値情報を説明するための図

350 しきい値情報

ICMP 50 回/秒 (1)
telnet 3 回/秒 (1)
ftp 3 回/秒 (1)
ICMP 80 回/秒 (2)
ftp 3 回/秒 (2)

【図9】

境界ルータ情報を説明するための図

152 境界ルータ情報

境界ルータ IP address#1
境界ルータ IP address#2
境界ルータ IP address#3
境界ルータ IP address#4

【図10】

接続ルータ情報を説明するための図

90 接続ルータ情報

自ルータ情報	接続ルータ情報
MAC address#1	接続ルータ IP address#1
VPI/VCI #1	接続ルータ IP address#2
入力ポート情報#1	接続ルータ IP address#3

【図11】

不正パケット情報を説明するための図

120 不正パケット情報

宛先 IP address
プロトコル種別
Port 番号
IP ヘッダー
MAC address または VPI/VCI または 入力ポート情報

【図12】

不正侵入レスポンスデータを説明するための図

不正侵入レスポンスデータ

140

宛先 IP address
自ルータ IP address
プロトコル種別
Port 番号
自ルータ AS 番号
IPアドレス種別 (不正発見/不正検知)

【図13】

しきい値情報の判定種別の要素を説明するための図

350

しきい値情報の判定種別

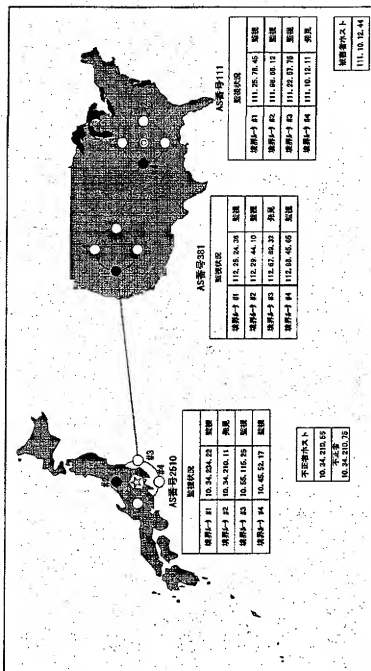
ICMP 50 回/秒 (1)
telnet 3 回/秒 (1)
Rp 3 回/秒 (1)
ICMP 50 回/秒 (3)
Rp 3 回/秒 (3)
...
...

判定種別部の要素

ICMP 50 回/秒 (1)	
以下の条件が全て AND 条件のとき 不正と判定する	
不正トワイ回数	50 回/秒
TTL 情報の種別	なし
パケット種別	ICMP エコー
宛先 IP 種別	なし
同一パケット判定	なし
投入パケット	なし
TTL 増減	あり
監視開始時刻	ALL
監視終了時刻	ALL
...	...
...	...
Telnet 3 回/秒 (1)	
以下の条件が全て AND 条件のとき 不正と判定する	
不正回数	3 回/秒
TTL 情報の種別	Telnet
パケット種別	なし
同一 IP 判定	あり
同一パケット判定	あり
投入パケット	ping
TTL 増減	あり
監視開始時刻	01:00
監視終了時刻	06:00
...	...
...	...

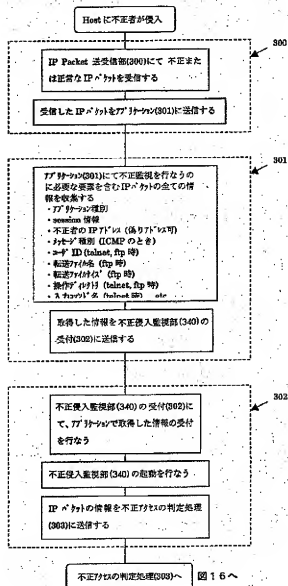
【図14】

不正侵入監視状況の表示例を示す図

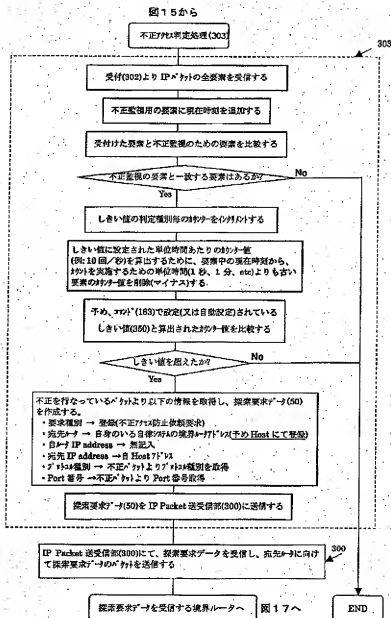


【図15】

被害者ホストコンピュータにおける不正者侵入時の
処理を示すフローチャート



被害者ホストコンピュータにおける不正者侵入時の処理を示すフローチャー



【図18】

境界ルータにおける不正者情報配布時の処理を示すフローチャート

図17から

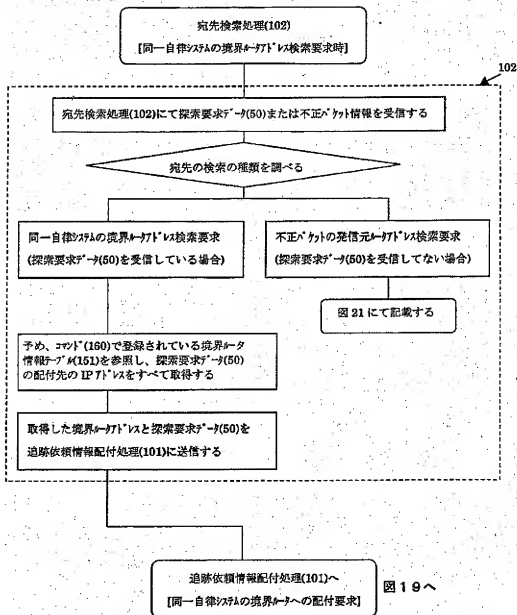
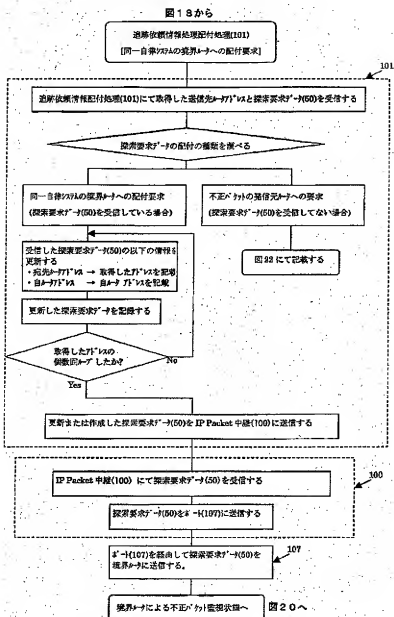


図19へ

【図19】

境界ルータにおける不正情報配布時の処理を示すフローチャート



【図20】

境界ルータにおける不正パケット監視時の処理を示すフローチャート

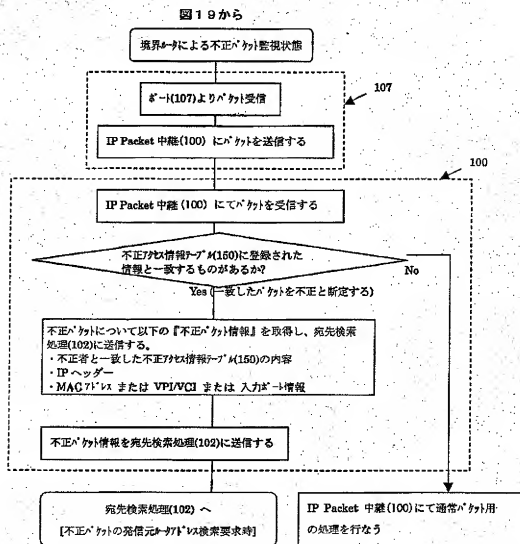
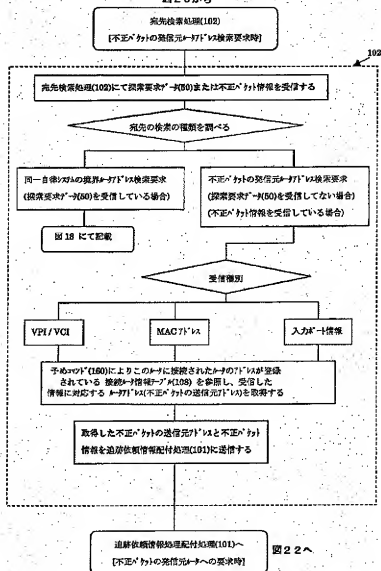


図21へ

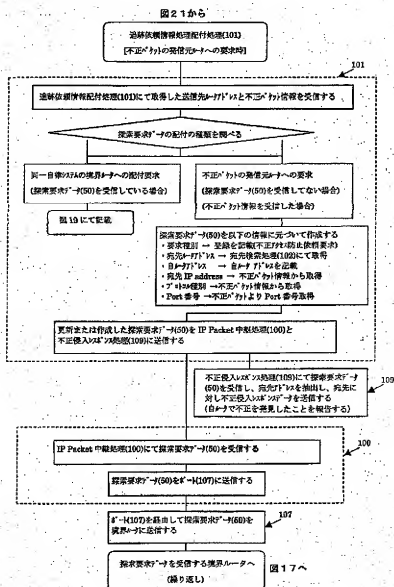
【図21】

境界ルータにおける不正パケット監視時の処理を示すフローチャート

図20から



境界ルータにおける不正パケット監視時の処理を示すフローチャート



フロントページの続き

- (72)発明者 田口 敦子
神奈川県横浜市港北区新横浜3丁目9番18
号富士通コミュニケーション・システムズ
株式会社内
- (72)発明者 近藤 竜夫
神奈川県横浜市港北区新横浜3丁目9番18
号富士通コミュニケーション・システムズ
株式会社内

- (72)発明者 木田 裕之
神奈川県横浜市港北区新横浜3丁目9番18
号富士通コミュニケーション・システムズ
株式会社内
Fターム(参考) 5B089 GA31 GB02 HA10 HB02 KA17
KB04 KB06 KB13 KC54
5K030 GA11 GA15 HA08 HC01 HD03
HD05 HD07 JA11 LC15 LD02
MA04 NR00